Why Hasn't Russia Hacked UK Political Parties?

This blog post was first posted to the International Centre for Security Analysis blog on the 17th May 2017.

What are the chances of a high-profile hacking of a UK political party between now and the General Election on 8 June? How helpful is it to try to quantify this probability? These are questions we asked ourselves recently at the International Centre for Security Analysis (ICSA).

On one hand, no previous UK general election has seen anything like the public release of hacked data that marred the November 2016 US presidential election. We have, after all, only just emerged from a major national referendum campaign with significant strategic implications, and a General Election the year before that, and neither of these campaigns were publicly blighted by hacking.

On the other hand, high-profile hacking episodes appear to be an emerging fact – the new normal? – in efforts to subvert the electoral processes of western democracies. And it's worth pointing out that 'fake news,' deception and information operations have a long pedigree in British politics - the October 1924 General Election and the Daily Mail's publication of the 'Zinoviev letter,' for example.

So, from one perspective, the question ought to be: 'Why haven't we already seen a similar dump of hacked emails in Britain?' We identified at least five hypotheses consistent with the (to date) absence of hacked data online:

1. UK political parties' cyber security is too strong;

2. UK political parties are too boring, so there isn't anything sufficiently useful or interesting to release;

3. State actors (like Russia) are less interested in the UK General Election than they were in the US or French presidential elections;

4. State actors are interested, but the snap election announcement left little time for a sustained operation to yield useful data;

5. A hacking operation is indeed underway, but these things take time and luck, maybe data has already been stolen, but the high-profile release is being held back until closer to election day.

In our view, points (1) - that UK party politics is unprecedentedly difficult as a target of cyber-attack - and (2) - that UK politicians are either too boring or too virtuous to leave behind embarrassing digital traces - can be discounted for several reasons. First, although we note that the National Cyber Security Centre has recently offered to assist political parties with cyber security issues, there have been several reports in recent years of UK politicians and their advisers using private webmail to discuss policy issues, suggesting that lax information security practices are not unknown in British politics, and regarding the 'boring virtue' of politicians, we simply point, as a counter example, to the continued existence of the tabloid press. To this we could obviously add several other rebuttals, such as that the absence of a real scandal is not a barrier to the creation of 'fake news' scandals (as is alleged to have been at least partly the case in France with the Macron leaks).

In our list of competing hypotheses, this leaves (3), (4) and (5): either the UK general election just isn't as important a target as the US or French presidential elections, or perhaps Theresa May's snap election announcement has made an effective cyber operation much more difficult to execute in the limited time, or on-going cyber-attacks are encountering the kind of difficulties that routinely beset them (e.g. reliance on waiting for a lucky break, like targeted users clicking on links in phishing emails), or, finally, the operation is on course, merely waiting for the moment of maximum impact to release a damaging cache of data.

These hypotheses are less easy to dismiss, especially with no access to the internal deliberations of hostile foreign intelligence services or the governments that direct their activities (for short-hand, we'll just say 'Russia' from now on, but there are clearly other

threats too). It is certainly possible that, with finite capacity, Russia prioritised resources to the known quantities of the US and French elections, meaning that – whatever the desirability of an attack on UK political parties – any operational activities are at an earlier phase, not well placed to intervene in a June General Election. (We read today, for example, that at least some apparently unsuccessful efforts were made earlier this year by an unknown hostile party to hack the private communications of a small number of MPs.) If we don't see a similar episode to the release of hacked emails in the US or France, one possible explanation would indeed be that the UK had a lower priority in the Russian operational pecking order during this time-period.

But there are several competing explanations that would also be consistent with this series of events.

For example, one competing scenario is that a concerted effort is indeed underway to hack political parties – presumably the Conservatives, as we don't really see what Russia would gain from damaging Jeremy Corbyn's electoral prospects. (But maybe Russian intelligence agencies are just very thorough, so who knows?) These operations are difficult, they take time, and they rely on a significant dose of good fortune, in the form of poor security practices by individuals or systemic shortcomings in the targeted organisations.

Just because we might not see a public release of hacked data during the election campaign, this wouldn't be conclusive evidence that an operation wasn't underway to hack British political parties. In fact, it wouldn't even mean that such an operation had been unsuccessful: Russia has the capability to intervene directly in elections by leaking covertly acquired information, but that doesn't mean that it always will do so. Traditionally, intelligence agencies collect information to inform the political masters' decision making: British political parties could indeed have been hacked, but the data might have been used secretly to inform officials in the Ministry of Foreign Affairs or the Presidential Administration, rather than to execute an overt intervention during the General Election campaign.

So, it's clear from this brief round-up that there are few hypotheses that could be completely dismissed should a leak fail to occur, excepting the hypothesis that Russia both has the information and intends to leak it. If they haven't done so by 8 June, we should at least be able to assume that they had reconsidered, but we couldn't take it as confirmation that no information was stolen, because such information could be used differently, to inform Russian decision-makers, or perhaps it could be stock-piled for a future, more overt use.

In analysing these competing hypotheses, we find it most plausible to believe that a combination of scenarios (4) and (5) is true: hacking is difficult, time-consuming and relies on luck, so whilst Russia might be keen to stage this kind of operation, the surprise of an early general election has made it even more difficult than usual to execute. This explanation could be amplified by elements of scenario (3), in the sense that resource- and other structural-constraints could mean that operations against the US and French presidential elections had had the effect of pushing the UK to a lower-tier targeting status over this time-period.

On this basis, especially in the apparent absence of similar operations during the 2015 General Election and 2016 referendum campaigns, we have reached the tentative conclusion that it is unlikely that a similar hack will occur before 8 June. How unlikely? Let's say we're as sure as we were that Donald Trump would lose the November 2016 presidential election. We certainly wouldn't recommend betting on our forecast. But in forecasting political events you've got to start somewhere, and then continuously revise those forecasts in the light of subsequent evidence.